Constructive interference based secure precoding

Constructive Interference Based Secure Precoding: A New Dimension in Physical Layer Security

Muhammad R. A. Khandaker, Christos Masouros, and Kai-Kit Wong

***Abstract*— Conventionally, interference and noise are treated as catastrophic elements in wireless communications. However, it has been shown recently that exploiting known interference constructively can contribute to signal detection ability at the receiving end. This paper exploits this concept to design artificial noise (AN) beamformers constructive to the intended receiver (IR) yet keeping AN disruptive to possible eavesdroppers (Eves). The scenario considered here is a multiple-input single-output wiretap channel with multiple Eves. This paper starts from AN design without any knowledge of Eve's CSI, builds with solutions with statistical CSI up to full CSI. Both perfect and imperfect channel information have been considered, in particular, with different extent of Eves' channel responses. The main objective is to improve the receive signal-to-interference and noise ratio at IR through exploitation of AN power in an attempt to minimize the total transmit power, while hindering detection at the Eves. Numerical simulations demonstrate that the proposed constructive AN precoding approach yields superior performance over conventional AN schemes in terms of transmit power. Critically, they show that, while the statistical constraints of conventional approaches may lead to instantaneous IR outages and security breaches from the Eves, the instantaneous constraints of our approach guarantee both IR performance and secrecy at every symbol period.**

***Index Terms*— Interference exploitation, constructive interference, physical layer security, robust design.**

I. Introduction

FIFTH-GENERATION (5G) wireless communication systems aim to achieve ultra-high spectral efficiency (SE) and orders-of-magnitude improved energy efficiency (EE). It is also expected that 5G networks will operate in multiple tiers deploying ultra-dense small-cell base stations (BSs), e.g., heterogeneous networks (HetNets). However, a major bottleneck in ultra-dense HetNets is the cross-tier and co-tier interference. In order to harvest the full potentials of 5G, developing sophisticated interference handling tools is a crying need at the moment.

Traditional approach to dealing with interference is to suppress the interference power in order to improve system performance [1], [2]. However, recent developments in interference exploitation techniques have revolutionised this traditional way of dealing with known interferences [3], [4]. Constructive interference (CI) precoding approaches suggest that interference power can even contribute to the received signal power if properly exploited [3]–[8]. This concept introduces a major breakthrough in designing wireless communication precoding when the interference is known at the transmitter. In particular, downlink beamforming design can be significantly improved by symbol-level precoding of known interferences [7]–[10]. With the knowledge of the users' data symbols and channel state information (CSI), the interference can be classified as constructive and destructive interferences. The theory and characterization criteria for constructive interference have been extensively studied in [3]–[10]. More recently, the concept has been exploited in energy harvesting systems [11], hybrid beamforming [12], cognitive radio networks [13] and massive MIMO systems [14]–[17]. The interference signals will be constructive to the desired signal if that moves the received symbols away from the decision thresholds of the constellation (e.g. real and imaginary axes for QPSK symbols) towards the direction of the desired symbol. In order to keep the angle of the interference signals aligned with the angle of the corresponding desired symbol, the transmit beamforming vectors need to be carefully designed.

The broadcast nature of wireless channels makes the communication naturally susceptible to various security threats. However, the security of wireless data transmission has traditionally been entrusted to key-based cryptographic methods at the network layer. Recently, physical-layer security (PLS) approaches have attracted a great deal of attention in the information-theoretic society since the accompanying techniques can afford an extra security layer on top of the traditional cryptographic approaches [18]–[24]. PLS exploits the channel-induced physical layer dynamics to provide information security. With appropriately designed coding and transmit precoding schemes in addition to the exploitation of any available CSI, PLS schemes enable secret communication over a wireless medium without the aid of an encryption key.

The extent of eavesdropper's CSI available at the transmitter plays a vital role in determining the corresponding optimal transmission scheme. If full CSI of all the links is available at the transmitter, then the spatial degrees of freedom (DoF) can be fully exploited to block interception [21]. However, it is generally very unrealistic in practice. In particular, it is almost impossible to obtain perfect eavesdroppers' CSI since eavesdroppers are often unknown malicious agents. The situation can further worsen if multiple eavesdroppers cooperate

Manuscript received August 31, 2017; revised January 24, 2018 and February 26, 2018; accepted February 26, 2018. Date of publication March 13, 2018; date of current version April 26, 2018. This work was supported in part by the Royal Academy of Engineering, U.K., and in part by the Engineering and Physical Sciences Research Council Project under Grant EP/M014150/1 and Grant EP/R007934/1. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Walid Saad. *(Corresponding author: Muhammad R. A. Khandaker.)*

The authors are with the Department of Electronic and Electrical Engineering, University College London, London WC1E 7JE, U.K. (e-mail: m.khandaker@ucl.ac.uk; c.masouros@ucl.ac.uk; kai-kit.wong@ucl.ac.uk).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIFS.2018.2815541

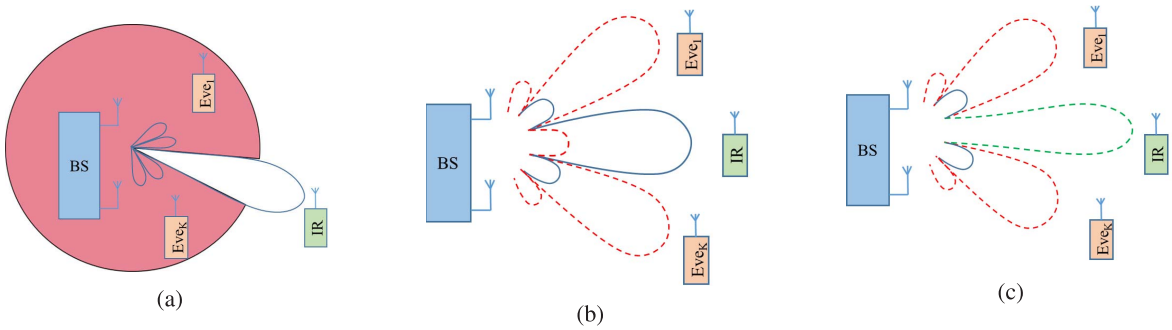

Fig. 1. Exploiting AN to boost secrecy performance. (a) Conventional isotropic AN. (b) Conventional spatially selective AN. (c) Constructive AN to boost received signal power.

in an attempt to maximize their interception through joint receive beamforming. Hence Li and Ma [21] and Khandaker and Wong [22], [23] considered robust secrecy beamforming design based on deterministic channel uncertainty models whereas [25] considered probabilistic robust design.

To make physical-layer secrecy viable, we usually need the legitimate user's channel condition to be better than the eavesdroppers'. However, this may not always be guaranteed in practice. To alleviate the dependence on the channel conditions, recent studies showed that the spatial DoF provided by multi-antenna technology can be exploited to degrade the reception of the eavesdroppers [20], [21]. A possible way to do this is transmit beamforming, which concentrates the transmit signal over the direction of the legitimate user while reducing power leakage to the eavesdroppers at the same time. Apart from this, a more operational approach is to send artificially generated noise signals to interfere the eavesdroppers deliberately [20]–[23]. Depending on the extent of eavesdroppers CSI available at the transmitter, different strategies can be applied to generate the optimal AN beams. If no eavesdroppers' CSI is available, then a popular design is the isotropic AN [20], where the message is transmitted in the direction of the intended receiver's channel, and spatio-temporal AN is uniformly spread on the orthogonal subspace of the legitimate channel (see Fig. 1a). This scheme guarantees that the intended receiver's (IR's) reception will be free from the interference by the AN, while the Eves' reception may be degraded by the AN. On the other hand, with knowledge of the eavesdroppers' CSI to some extent, one can block the eavesdroppers' interception more efficiently by generating spatially selective AN (see Fig. 1b) [21], [22]. More recently, an antenna array based directional modulation scheme (DM) has been studied which enhances security through adjusting the amplitude and phase of the transmit signal along a specific direction by varying the length of the reflector antennas for each symbol while scrambling the symbols in other directions [26]–[29]. Note that the AN is in general disruptive to the legitimate receivers as well, in the above (conventional) schemes. This creates serious problems particularly when exact CSI can not be obtained. This motivates us to rethink the role of interferences as well as the AN.

In this paper, we exploit the knowledge of interference readily available at the transmitter for improving security in wireless systems [30]. In this context, we redesign AN signals in the form of constructive interference to the IR while keeping AN disruptive to potential Eves. We consider a multiple-input single-output (MISO) downlink system in the presence of multiple Eves as shown in Fig. 1c. We aim at minimizing the total transmit power while boosting the received SINR at the IR as well as degrading the Eves' SINR below certain threshold. The benefits of constructive interference-based AN precoding scheme is twofold compared to conventional AN-based physical-layer security schemes considered in [20]–[23]. Firstly, the constructive AN will boost the receive SINR at the IR as opposed to the conventional AN-based schemes which attempt to suppress AN signals along the direction of the IR. Secondly, to achieve a predefined level of SINR at the IR, constructive interference based precoding scheme requires lower power compared to conventional AN precoding, thus diminishing inter-user as well as inter-cell interferences. Depending on the extent of eavesdropping information available at the transmitter, we propose different constructive interference based secure precoding schemes. In particular, we consider different scenarios with i) no eavesdropping CSI, ii) Eves' statistical CSI, and iii) Eves' full CSI, perfect and imperfect. Numerical simulations demonstrate that the proposed constructive AN precoding approaches yield superior performance over conventional schemes in terms of transmit power. For clarity, the contributions are summarized below:

1) We first consider the case when no information is available about the eavesdroppers, with perfect IR CSI. We propose constructive interference based AN design for the IR as opposed to the conventional isotropic AN design onto the null space of the IR.
2) Then, we design a secure precoding scheme with eavesdroppers' CSI statistics available, such that the AN is constructive to the IR while satisfying statistical eavesdropping constraints thus reducing the required transmit power for given performance and secrecy requirements.
3) Next, when full CSI is available, this allows the design to move one step further to satisfy instantaneous SINR constraints at all nodes such that the AN is constructive to the IR and destructive to Eves, further impeding signal detection at the Eves and reducing the required transmit power to guarantee predefined security.

4) We further develop a computationally efficient algorithm for the constructive AN precoding scheme based on projected gradient approach.
5) Finally, we design worst-case robust secure precoders in the presence of imperfect CSI of all the nodes.

In all cases, the proposed schemes outperform the conventional AN-aided secure precoding schemes. Note that only the full CSI case has been considered in [30] without proposing any efficient solver.

The rest of this paper is organized as follows. In Section II, the model of a secret MISO downlink system is introduced. Section III demonstrates how constructive interference precoding scheme boosts receive SINR. The SINR-constrained power minimization problems with a) no Eves' CSI, b) Eves' statistical CSI, and c) all-perfect CSI have been studied in Sections IV, V, and VI, respectively. In Section VII, we develop an efficient solver for the constructive-destructive precoding problem. On the other hand, robust constructive AN precoding has been designed in Section VIII. Section IX presents the simulation results that justify the significance of the proposed algorithms under various scenarios. Concluding remarks are provided in Section X.

II. System Model

Following [31], we consider a MISO downlink system where the transmitter (BS) equipped with N_{T} transmit antennas intends to transmit a secret message to the IR in the presence of K possible eavesdroppers. The IR and the Eves are all equipped with a single antenna for notational simplicity, while our techniques can be readily extended to multi-antenna receivers. In order to confuse the Eves, the BS injects AN signals into the secret message in an attempt to reduce the receive SINRs at the Eves. Thus the received signal at the IR and those at the Eves are given, respectively, by y_{d} and $y_{\mathrm{e},k}$:

$$y_{\mathrm{d}} = \mathbf{h}_{\mathrm{d}}^T \mathbf{x} + n_{\mathrm{d}}, \tag{1}$$

$$y_{\mathrm{e},k} = \mathbf{h}_{\mathrm{e},k}^T \mathbf{x} + n_{\mathrm{e},k}, \quad \text{for } k = 1, \ldots, K, \tag{2}$$

where $\mathbf{h}_{\mathrm{d}}$ and $\mathbf{h}_{\mathrm{e},k}$ are the complex channel vectors between the BS and the IR and between the BS and the kth Eve, respectively, $n_{\mathrm{d}} \sim \mathcal{CN}(0, \sigma_{\mathrm{d}}^2)$ and $n_{\mathrm{e},k} \sim \mathcal{CN}(0, \sigma_{\mathrm{e}}^2)$ are the additive Gaussian noises at the IR and the kth Eve, respectively. The BS chooses $\mathbf{x}$ as the sum of information beamforming vector $\mathbf{b}_{\mathrm{d}} s_{\mathrm{d}}$ and the AN vector $\mathbf{z}$ such that the baseband transmit signal vector is

$$\mathbf{x} = \mathbf{b}_{\mathrm{d}} s_{\mathrm{d}} + \mathbf{z}, \tag{3}$$

where $s_{\mathrm{d}} = d e^{j\phi_{\mathrm{d}}}$ is the confidential information-bearing symbol for the IR, d indicates the constant amplitude and ϕ_{d} is the phase.

Accordingly, the received SINR at the IR is given by

$$\gamma_{\mathrm{d}} = \frac{\left|\mathbf{h}_{\mathrm{d}}^T \mathbf{b}_{\mathrm{d}}\right|^2}{\left|\mathbf{h}_{\mathrm{d}}^T \mathbf{z}\right|^2 + \sigma_{\mathrm{d}}^2}, \tag{4}$$

and that at the kth Eve is given by

$$\gamma_{\mathrm{e},k} = \frac{\left|\mathbf{h}_{\mathrm{e},k}^T \mathbf{b}_{\mathrm{d}}\right|^2}{\left|\mathbf{h}_{\mathrm{e},k}^T \mathbf{z}\right|^2 + \sigma_{\mathrm{e}}^2}, \forall k. \tag{5}$$

The transmit signal $\mathbf{x}$ can also be expressed as

$$\mathbf{x} = \mathbf{b}_{\mathrm{d}} s_{\mathrm{d}} + \mathbf{z} e^{-j\phi_{\mathrm{d}}} s_{\mathrm{d}} \tag{6}$$

Assuming constant envelop[1] $d = 1$, the instantaneous transmit power is given by

$$P_{\mathrm{T}} = \|\mathbf{b}_{\mathrm{d}} s_{\mathrm{d}} + \mathbf{z}\|^2 = \left\|\mathbf{b}_{\mathrm{d}} + \mathbf{z} e^{-j\phi_{\mathrm{d}}}\right\|^2. \tag{7}$$

In the following, we design precoding schemes for instantaneous transmit power minimization exploiting known interference (AN in this case) power.

III. Constructive Interference Precoding Technique

Recent advances in interference exploitation have demonstrated that constructive interference precoding techniques can significantly improve receive SINR thus reducing signal detection errors. The theory and characterization criteria for constructive interference have been extensively studied first in the context of code division multiple access (CDMA) systems [9], [32]–[34], and more recently to MIMO systems in [3]–[6] and [8]. To avoid repetition, we refer the readers to the above works for the details, while here we employ this concept directly to design our new optimization problems. We will actively exploit interference (AN in this case) constructively for the IR to reduce the required power for a given SINR threshold, while guaranteeing the secrecy constraint for the Eves. The AN signal will be constructive to the received signal at the IR if that moves the received symbols away from the decision thresholds of the constellation (e.g. real and imaginary axes for QPSK symbols in Fig. 2a).[2] Hence we intend to keep the angle of that part aligned with the angle of the corresponding desired symbol s_{d} by appropriately designing the transmit beamforming vectors. We can do so by pushing the decision symbols towards the constructive regions of the modulation constellation, denoted by the green shaded areas (cf. Fig. 2a).

For constructive precoding, the AN signals received at the IR are not suppressed or nullified in contrast to the conventional use of AN [21], [22], [31], rather optimized instantaneously such that they contribute to the received signal power. If the AN signals can be aligned with the data symbols s_{d} by properly designing the beamforming precoding vectors, then the AN signals will contribute constructively. Accordingly, it has been shown in [6] and [8] that the receive SINR (4) at the IR can be rewritten as

$$\gamma_{\mathrm{d}} = \frac{\left|\mathbf{h}_{\mathrm{d}}^T \mathbf{b}_{\mathrm{d}} + \mathbf{h}_{\mathrm{d}}^T \mathbf{z} e^{-j\phi_{\mathrm{d}}}\right|^2}{\sigma_{\mathrm{d}}^2}. \tag{8}$$

Note that the receive SINR at the IR has actually become SNR after constructive AN precoding. However, the SINR at the kth

[1] Without loss of generality, we assume $d = 1$ in this paper for notational convenience. However, our analyses are valid for any value of d.

[2] Although we selected QPSK as a representative modulation scheme for exposition, the proposed algorithms and our analyses apply to any PSK modulation scheme. Moreover, the proposed methodologies can be straightforwardly adapted for multi-level modulation schemes like QAM following the analyses in [12].

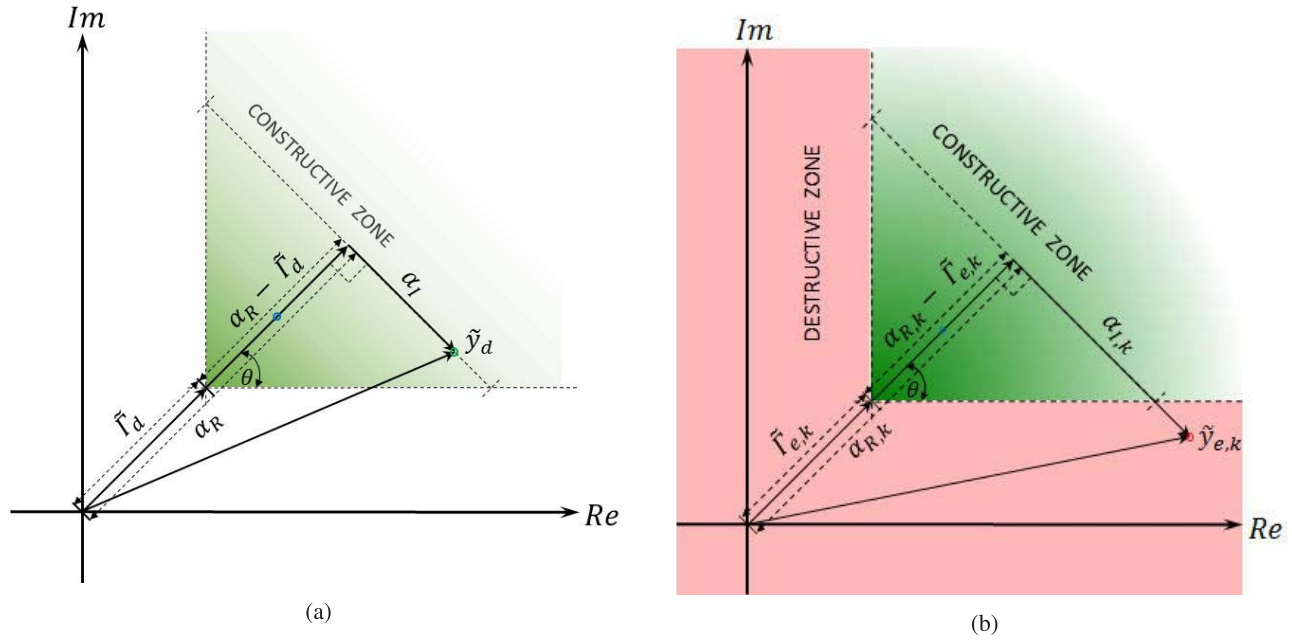

Fig. 2. Exploiting constructive and destructive AN for QPSK symbols. (a) Constructive AN design for the legitimate receiver. Constructive interference power pushes the decision symbols towards the constructive regions of the modulation constellation, denoted by the green shaded areas. (b) Destructive AN design for the eavesdropper. Destructive AN pushes the received signal at the Eves away from the decision thresholds (red zone).

Eve remains the same as in (5) since no AN signal has been made constructive to the Eves.

Thus exploiting AN power constructively, the instantaneous SINR constraint at the IR can be formulated as the following system of constraints

$$\angle\left(\mathbf{h}_{\mathrm{d}}^T\mathbf{b}_{\mathrm{d}} + \mathbf{h}_{\mathrm{d}}^T\mathbf{z}e^{-j\phi_{\mathrm{d}}}\right) = \angle\left(s_{\mathrm{d}}\right) \tag{9a}$$

$$\frac{\Re\left\{\mathbf{h}_{\mathrm{d}}^T\left(\mathbf{b}_{\mathrm{d}} + \mathbf{z}e^{-j\phi_{\mathrm{d}}}\right)\right\}^2}{\sigma_{\mathrm{d}}^2} \geq \Gamma_{\mathrm{d}}, \tag{9b}$$

where Γ_{d} is the SINR requirement for correct detection at the IR, $\Re\{x\}$ indicates the real part of the complex number x and $\angle x$ denotes the corresponding angle. Note that the phases of the AN signals in (9b) have been shifted by the phase of the desired symbol s_{d}. The constraint (9a) imposes that the AN fully aligns with the phase of the symbol of interest s_{d} at the IR, whereas the constraint (9b) guarantees that the constructively precoded AN signals can adequately satisfy the SINR requirement at the IR. We note that this signal alignment will only hold for the structure of the IR's channel $\mathbf{h}_{\mathrm{d}}$, while there will be no such alignment for the Eves' channels $\mathbf{h}_{\mathrm{e},k}$.

Essentially, the angular constraint (9a) is a very strict constraint. But exploiting the concept of constructive interference, we can actually relax this constraint without losing any optimality which results in a larger feasible region. Let us denote $\tilde{y}_{\mathrm{d}} \triangleq \mathbf{h}_{\mathrm{d}}^T\left(\mathbf{b}_{\mathrm{d}} + \mathbf{z}e^{-j\phi_{\mathrm{d}}}\right)$ as the received signal ignoring the AWGN at the IR, with constructive AN injected, and α_{R} and α_{I} as the abscissa and the ordinate of the phase-adjusted signal $\tilde{y}_{\mathrm{d}}$, respectively. Applying basic geometric principles to Fig. 2a, the constraints in (9) can be equivalently represented as

$$\Im\left\{\mathbf{h}_{\mathrm{d}}^T\left(\mathbf{b}_{\mathrm{d}} + \mathbf{z}e^{-j\phi_{\mathrm{d}}}\right)\right\} = 0 \tag{10a}$$

$$\Re\left\{\mathbf{h}_{\mathrm{d}}^T\left(\mathbf{b}_{\mathrm{d}} + \mathbf{z}e^{-j\phi_{\mathrm{d}}}\right)\right\} \geq \sigma_{\mathrm{d}}\sqrt{\Gamma_{\mathrm{d}}}, \tag{10b}$$

where $\Im\{x\}$ indicates the imaginary part of the complex number x. However, it can be observed from Fig. 2a that the AN contaminated received signal $\tilde{y}_{\mathrm{d}}$ does not necessarily need to strictly align the angle of the desired signal. That is, $\tilde{y}_{\mathrm{d}}$ lays on the constructive zone of the desired symbol s_{d} as long as the following condition is satisfied

$$-\theta \leq \phi_{\mathrm{d}} \leq \theta, \quad \text{i.e.,} \quad \frac{|\alpha_{\mathrm{I}}|}{\alpha_{\mathrm{R}} - \tilde{\Gamma}_{\mathrm{d}}} \leq \tan\theta, \tag{11}$$

where $\tilde{\Gamma}_{\mathrm{d}} \triangleq \sigma_{\mathrm{d}}\sqrt{\Gamma_{\mathrm{d}}}$ and $\theta = \pi/M$, M is the constellation size. Thus the strict angle constraint (10a) can be relaxed as

$$\left|\Im\left\{\mathbf{h}_{\mathrm{d}}^T\left(\mathbf{b}_{\mathrm{d}} + \mathbf{z}e^{-j\phi_{\mathrm{d}}}\right)\right\}\right| \leq \left(\Re\left\{\mathbf{h}_{\mathrm{d}}^T\left(\mathbf{b}_{\mathrm{d}} + \mathbf{z}e^{-j\phi_{\mathrm{d}}}\right)\right\} - \sigma_{\mathrm{d}}\sqrt{\Gamma_{\mathrm{d}}}\right)\tan\theta. \tag{12}$$

Note that the relaxed angular constraint (12) allows a larger feasibility region (entire green zone in Fig. 2a). Interestingly, the QoS constraint Γ_{d} is embedded in (12). Hence we do not need to explicitly impose it in the optimization procedure. In the following, we exploit this constructive interference constraint in various scenarios depending on the extent of CSI available at the transmitter.

IV. Unknown Eavesdroppers' CSI

In many practical scenarios, it is often difficult to obtain any information about the eavesdroppers' CSI, or it may even be impractical to assume that the transmitter is aware

of the presence of an Eve at all. However, communication secrecy can still be improved by transmitting AN. In order to ensure secure communication in such cases, a reasonable approach is to allocate minimum resources necessary to obtain a certain level of quality-of-service (QoS) for the IR, and devote all other resources to making interception of the signal more difficult. However, the downside is that the secrecy performance of such a scheme cannot be guaranteed. The eavesdropper's received signal at a defined location can be of better quality than the IR's thus allowing information leakage. In this section, we study conventional and interference exploitation approaches to make the probability of such an event as low as possible when no information is available about the potential eavesdroppers.

A. Conventional Isotropic AN Design

A conventional approach is to allocate a fraction ρ of the available transmit power P_t for transmitting the confidential message signal to achieve the minimum required SINR at the IR such that the IR experiences no interference at all [31], [35]. The remaining power is distributed isotropically onto the null space of the legitimate channel to yield as much interference as possible. Formally, the optimization problem can be represented as

$$\min_{\mathbf{b}_\mathrm{d},\mathbf{z}} \ \rho P_t \left\|\mathbf{b}_\mathrm{d}\right\|^2 + (1-\rho)P_t \left\|\mathbf{z}\right\|^2 \tag{13a}$$

$$\text{s.t.} \ \frac{\rho P_t \left|\mathbf{h}_\mathrm{d}^T \mathbf{b}_\mathrm{d}\right|^2}{(1-\rho)P_t \left|\mathbf{h}_\mathrm{d}^T \mathbf{z}\right|^2 + \sigma_\mathrm{d}^2} \geq \Gamma_\mathrm{d}, \tag{13b}$$

$$= \mathbf{\Pi}^{\perp}\mathbf{h}_\mathrm{d}, \tag{13c}$$

where $\mathbf{\Pi}^{\perp} = \mathbf{I}_{N_\mathrm{T}} - \mathbf{h}_\mathrm{d}\mathbf{h}_\mathrm{d}^H/\|\mathbf{h}_\mathrm{d}\|^2$ is the orthogonal complement projection matrix of $\mathbf{h}_\mathrm{d}$. The optimal ρ is chosen such that the legitimate IR's SINR requirement in (13b) is just met, i.e.,

$$\frac{\rho P_t \left|\mathbf{h}_\mathrm{d}^T \mathbf{b}_\mathrm{d}\right|^2}{\sigma_\mathrm{d}^2} = \Gamma_\mathrm{d}, \tag{14}$$

which yields $\rho = \frac{\sigma_\mathrm{d}^2 \Gamma_\mathrm{d}}{P_t}$, with $\mathbf{b}_\mathrm{d} = \frac{\mathbf{h}_\mathrm{d}}{\|\mathbf{h}_\mathrm{d}\|^2}$, and $\mathbf{W}_\mathrm{n} = (1-\rho)P_t\mathbf{\Pi}^{\perp}$ is the AN covariance matrix [31], [35]. Essentially, if the QoS requirements in problem (13) are too demanding, then the problem will be infeasible. Hence the network designer must set the design parameters realistically such that the constraint (13b) is reachable within the given power budget P_t. However, this solution may not in general yield the best possible SINR for the IR.

B. Constructive Isotropic AN Design

In practice, the conventional approach of allocating minimum power for information transmission and maximum power for AN transmission may not always result in the maximum possible secrecy performance. Instead, allowing some extent of AN to leak to the IR in a constructive-interference fashion, will contribute to the received SINR at the IR [6], as discussed in Section III.

In this section, we take the conventional isotropic beamforming approach one step forward by exploiting AN constructively for the IR to reduce the required power for a given SINR threshold, thanks to the perfect knowledge of IR's CSI. We do this by optimizing the transmitted signal part ($\mathbf{x}$ in (1)), which comprises of the desired symbol and the AN signals. The direct benefit is that the IR's SINR requirement is satisfied to equality investing relatively lower power for information transmission and the additionally saved power could be allocated to spreading the AN isotropically within given power budget. This should further help confusing any potential eavesdropper. Thus considering the constructive form of the IR's SINR, as discussed in Section III, we formulate the instantaneous total power minimization problem as

$$\mathbf{P1}: \ \min_{\mathbf{b}_\mathrm{d},\mathbf{z}} \ \left\|\sqrt{\rho P_t}\mathbf{b}_\mathrm{d} + \sqrt{(1-\rho)P_t}\mathbf{z}e^{-j\phi_\mathrm{d}}\right\|^2 \tag{15a}$$

$$\text{s.t.} \ \left|\Im\left(\mathbf{h}_\mathrm{d}^T\left(\sqrt{\rho P_t}\mathbf{b}_\mathrm{d} + \sqrt{(1-\rho)P_t}\mathbf{z}e^{-j\phi_\mathrm{d}}\right)\right)\right|$$

$$\leq \left(\Re\left(\mathbf{h}_\mathrm{d}^T\left(\sqrt{\rho P_t}\mathbf{b}_\mathrm{d} + \sqrt{(1-\rho)P_t}\mathbf{z}e^{-j\phi_\mathrm{d}}\right)\right) - \sqrt{\sigma_\mathrm{d}\Gamma_\mathrm{d}}\right)\tan\theta, \tag{15b}$$

$$\|\mathbf{z}\|^2 \geq P_\mathrm{n}. \tag{15c}$$

Note that problem (15) adopts the instantaneous transmit power (including data symbols) as the objective to minimize, as opposed to the average transmit power in conventional optimization framework (13). The relaxed angular constraint (15b) allows a larger feasibility region, which results in a lower minimum transmit power as we will observe in the simulation results of Section IX. It is also important to note that the constraint (15c) guarantees the minimum AN transmitted power and P_n is the guaranteed minimum noise transmit level.[3] Since there is no information available about the eavesdropping channels, the constraint (15c) plays an important role in secure beamforming design. Since the optimization objective is to minimize the total transmit power, the optimal solver would allocate almost zero power to the AN signal without this constraint. While this is desirable for saving power, it would not disrupt the eavesdroppers' reception as required. Thus the constraint (15c) plays an important role in jamming the eavesdroppers' channel yet transmitting at a lower power compared to the conventional isotropic AN scheme introduced in the previous subsection. However, the problem (15) is still not convex due to the non-convex constraint (15c) and the coupling of the optimization variables. But we can convexify the constraint (15c) by reformulating it as a geometric mean constraint (GMC) [36]. The problem is then solved for given ρ. The optimal ρ can be obtained performing a one-dimensional searching.

V. Statistical Eavesdropper CSI

Suppose that the transmitter does not know the instantaneous CSI of the eavesdroppers, but can obtain the CSI statistics from long-term measures. Unlike traditional channel training where pilot signals are transmitted to obtain CSI before actual data transmission begins, statistical CSI can be estimated based on historical transmissions. In this section,

[3] It is assumed that the system designer can set this threshold such that the noise level makes correct decoding by the eavesdroppers extremely difficult. This may vary depending on the system requirements.

we assume that the time average can equivalently approximate the ensemble average due to the ergodicity of random channels. For the legitimate IR's MISO channel, we suppose that the transmitter obtains the perfect CSI through feedback transmission from the receiver. Let us now define the kth Eve's channel correlation matrix as

$$\mathbf{R}_{\mathrm{e},k} = \mathbb{E}\left\{\mathbf{h}_{\mathrm{e},k}\mathbf{h}_{\mathrm{e},k}^H\right\} = \boldsymbol{\mu}_{\mathrm{e},k}\boldsymbol{\mu}_{\mathrm{e},k}^H + \mathbf{Q}_{\mathrm{e},k}, \quad k = 1, \cdots, K, \tag{16}$$

where $\mathbb{E}\{\cdot\}$ indicates statistical expectation, $\boldsymbol{\mu}_{\mathrm{e},k}$ is the mean and $\mathbf{Q}_{\mathrm{e},k}$ is the covariance of $\mathbf{h}_{\mathrm{e},k}$. In fact, the covariance $\mathbf{Q}_{\mathrm{e},k}$, $\forall k$, indicates the level of CSI uncertainty in second-order statistics sense. For ease of exposition, let us now assume that the eavesdroppers' channels have white covariances, i.e.,

$$\mathbf{R}_{\mathrm{e},k} = \boldsymbol{\mu}_{\mathrm{e},k}\boldsymbol{\mu}_{\mathrm{e},k}^H + \sigma_{\mathrm{h},k}^2\mathbf{I}_{N_\mathrm{T}}, \forall k, \tag{17}$$

with $\sigma_{\mathrm{h},k}^2 \geq 0$. Obviously, $\sigma_{\mathrm{h},k}^2 = 0$ indicates the perfect CSI case which we elaborate in Section VI. The rest of the analyses in this section is therefore based on the assumption that $\sigma_{\mathrm{h},k}^2 > 0$, i.e., the correlation matrix $\mathbf{R}_{\mathrm{e},k}$ is a nonsingular positive definite matrix.

A. Statistical CSI Based Conventional Secure Precoding

With the knowledge of the eavesdroppers' CSI to some extent, one can block the eavesdroppers' interception more efficiently by generating spatially selective AN. The design objective is still power minimization under SINR constraint at the IR, however, with additional secrecy constraints against eavesdropping. In order to satisfy these secrecy requirements, conventional secrecy power minimization problem with Eves' CSI statistics is formulated as [31]

$$\min_{\mathbf{W}_\mathrm{d},\mathbf{W}_\mathrm{n}} \ \mathrm{Tr}(\mathbf{W}_\mathrm{d}) + \mathrm{Tr}(\mathbf{W}_\mathrm{n}) \tag{18a}$$

$$\text{s.t.} \ \frac{1}{\Gamma_\mathrm{d}}\mathrm{Tr}(\mathbf{W}_\mathrm{d}\mathbf{R}_\mathrm{d}) - \mathrm{Tr}(\mathbf{R}_\mathrm{d}\mathbf{W}_\mathrm{n}) \geq \sigma_\mathrm{d}^2, \tag{18b}$$

$$\frac{1}{\Gamma_{e,k}}\mathrm{Tr}(\mathbf{W}_\mathrm{d}\mathbf{R}_{\mathrm{e},k}) - \mathrm{Tr}(\mathbf{R}_{\mathrm{e},k}\mathbf{W}_\mathrm{n}) \leq \sigma_\mathrm{e}^2, \quad \forall k, \tag{18c}$$

$$\mathbf{W}_\mathrm{d} \succeq \mathbf{0}, \quad \mathbf{W}_\mathrm{n} \succeq \mathbf{0}, \ \mathrm{rank}(\mathbf{W}_\mathrm{d}) = 1, \tag{18d}$$

where $\mathbf{R}_\mathrm{d} \triangleq \mathbf{h}_\mathrm{d}\mathbf{h}_\mathrm{d}^H$, $\mathbf{W}_\mathrm{d} \triangleq \mathbf{b}_\mathrm{d}\mathbf{b}_\mathrm{d}^H$, $\mathbf{W}_\mathrm{n} \triangleq \mathbf{z}\mathbf{z}^H$, and $\Gamma_{\mathrm{e},k}$ is the secrecy threshold for the k-th Eve. Conventionally, the nonconvex rank constraint is dropped so that the relaxed problem can be solved using existing solvers [37]. Interestingly, it has been proven in [22] and [31] that for a practically representative class of scenarios, the original problem can be solved optimally. Although the solutions proposed in [22] and [31] are optimal from stochastic viewpoint, the hidden power in the AN signals has been treated as harmful for the desired information, and hence, either nullified or suppressed. In the following subsection, we endeavour to develop a precoding scheme exploiting the AN power constructively for the desired signal at the IR yet keeping it disruptive to the Eves.

B. Statistical CSI Based Constructive AN Precoding

With perfect CSI of the IR and statistical mean and covariance of the eavesdroppers' channels available at the transmitter, one can design the transmit precoding and the AN beamforming more effectively. In particular, we aim at designing the precoders such that the AN is constructive to the IR while maintaining the conventional secrecy constraints to the Eves. As such, the plain constructive interference based secure transmit precoding optimization problem with statistical Eves' CSI can be formulated as

$$\min_{\mathbf{b}_\mathrm{d},\mathbf{z}} \ \left\|\mathbf{b}_\mathrm{d} + \mathbf{z}e^{-j\phi_\mathrm{d}}\right\|^2 \tag{19a}$$

$$\text{s.t.} \ \left|\Im\left\{\mathbf{h}_\mathrm{d}^T\left(\mathbf{b}_\mathrm{d} + \mathbf{z}e^{-j\phi_\mathrm{d}}\right)\right\}\right| \leq \left(\Re\left\{\mathbf{h}_\mathrm{d}^T \times \left(\mathbf{b}_\mathrm{d} + \mathbf{z}e^{-j\phi_\mathrm{d}}\right)\right\} - \sigma_\mathrm{d}\sqrt{\Gamma_\mathrm{d}}\right)\tan\theta, \tag{19b}$$

$$\frac{\mathbf{b}_\mathrm{d}^H\mathbf{R}_{\mathrm{e},k}\mathbf{b}_\mathrm{d}}{\mathbf{z}^H\mathbf{R}_{\mathrm{e},k}\mathbf{z} + \sigma_\mathrm{e}^2} \leq \Gamma_{\mathrm{e},k}, \quad \forall k. \tag{19c}$$

Note that the global optimal solution to the problem (19) can not be guaranteed due to the secrecy constraint (19c) with statistical channel knowledge only. Manipulating this constraint, the problem (19) can be efficiently solved using convex optimization toolboxes, e.g., CVX [37]. Using the definition of $\mathbf{W}_\mathrm{d} = \mathbf{b}_\mathrm{d}\mathbf{b}_\mathrm{d}^H$ and $\mathbf{W}_\mathrm{n} \triangleq \mathbf{z}\mathbf{z}^H$, one can express the secrecy constraint (19c) as a linear matrix inequality (LMI). Thus the problem (19) can be expressed as

$$\mathbf{P2}: \ \min_{\mathbf{b}_\mathrm{d},\mathbf{z}} \ \left\|\mathbf{b}_\mathrm{d} + \mathbf{z}e^{-j\phi_\mathrm{d}}\right\|^2 \tag{20a}$$

$$\text{s.t.} \ \left|\Im\left\{\mathbf{h}_\mathrm{d}^T\left(\mathbf{b}_\mathrm{d} + \mathbf{z}e^{-j\phi_\mathrm{d}}\right)\right\}\right| \leq \left(\Re\left\{\mathbf{h}_\mathrm{d}^T \times \left(\mathbf{b}_\mathrm{d} + \mathbf{z}e^{-j\phi_\mathrm{d}}\right)\right\} - \sigma_\mathrm{d}\sqrt{\Gamma_\mathrm{d}}\right)\tan\theta, \tag{20b}$$

$$\begin{bmatrix} \mathrm{tr}\left(\mathbf{R}_{\mathrm{e},k}\mathbf{W}_\mathrm{d}\right) - \mathrm{tr}\left(\mathbf{R}_{\mathrm{e},k}\mathbf{W}_\mathrm{n}\right) & \sigma_\mathrm{e} \\ \sigma_\mathrm{e} & 1 \end{bmatrix} \succeq \mathbf{0}, \quad \forall k, \tag{20c}$$

$$\begin{bmatrix} \mathbf{W}_\mathrm{d} & \mathbf{b}_\mathrm{d} \\ \mathbf{b}_\mathrm{d} & 1 \end{bmatrix} \succeq \mathbf{0} \quad \mathbf{W}_\mathrm{n} \succeq \mathbf{0}. \tag{20d}$$

Note that the constraint (20d) takes care of the rank constraint[4] on $\mathbf{W}_\mathrm{d}$.

VI. Secure Precoding With Full CSI

In this section, we assume that perfect CSI of all the receivers (including potential eavesdroppers) is available at the transmitter. This assumption is valid for scenarios where the eavesdroppers are also active users of the system, possibly for different services. In such cases, the transmitter can estimate the CSI from the active eavesdroppers' transmission.

A. Conventional Secure Precoding With Full CSI

With perfect CSI of both the IR and the Eves, the conventional power minimization problem with QoS constraints is

[4]The problem (20) yields a unit-rank $\mathbf{W}_\mathrm{d}$ in all Monte Carlo simulations we performed in Section IX.

formulated as

$$\mathbf{P}-\mathbf{Conv}: \quad \min_{\mathbf{b}_\mathrm{d},\mathbf{z}} \ \|\mathbf{b}_\mathrm{d}\|^2+\|\mathbf{z}\|^2 \tag{21a}$$

$$\text{s.t.} \ \frac{\left|\mathbf{h}_\mathrm{d}^T\mathbf{b}_\mathrm{d}\right|^2}{\left|\mathbf{h}_\mathrm{d}^T\mathbf{z}\right|^2+\sigma_\mathrm{d}^2}\geq\Gamma_\mathrm{d}, \tag{21b}$$

$$\frac{\left|\mathbf{h}_{\mathrm{e},k}^T\mathbf{b}_\mathrm{d}\right|^2}{\left|\mathbf{h}_{\mathrm{e},k}^T\mathbf{z}\right|^2+\sigma_\mathrm{e}^2}\leq\Gamma_{\mathrm{e},k}, \quad \forall k. \tag{21c}$$

The power minimization problem has been solved in many existing works for different scenarios [21], [31]. One conventional approach is to reformulate problem (21) as the following semidefinite program (SDP) after relaxing the rank constraint

$$\min_{\mathbf{W}_\mathrm{d},\mathbf{W}_\mathrm{n}} \ \mathrm{Tr}(\mathbf{W}_\mathrm{d})+\mathrm{Tr}(\mathbf{W}_\mathrm{n}) \tag{22a}$$

$$\text{s.t.} \ \frac{1}{\Gamma_\mathrm{d}}\mathrm{Tr}(\mathbf{W}_\mathrm{d}\mathbf{R}_\mathrm{d})-\mathrm{Tr}(\mathbf{R}_\mathrm{d}\mathbf{W}_\mathrm{n})\geq\sigma_\mathrm{d}^2, \tag{22b}$$

$$\frac{1}{\Gamma_{e,k}}\mathrm{Tr}(\mathbf{W}_\mathrm{d}\mathbf{R}_{\mathrm{e},k})-\mathrm{Tr}(\mathbf{R}_{\mathrm{e},k}\mathbf{W}_\mathrm{n})\leq\sigma_\mathrm{e}^2, \quad \forall k, \tag{22c}$$

$$\mathbf{W}_\mathrm{d}\succeq\mathbf{0}, \quad \mathbf{W}_\mathrm{n}\succeq\mathbf{0}. \tag{22d}$$

However, since the Eves' CSI is now perfectly known, the corresponding channel correlation matrices are obtained as $\mathbf{R}_{\mathrm{e},k}=\mathbf{h}_{\mathrm{e},k}\mathbf{h}_{\mathrm{e},k}^H$. The reformulated problem (22) can be optimally solved using CVX [21], [31].

B. Constructive AN-Based Secure Precoding

In this section, our attempt is to further improve the secrecy performance utilizing the full knowledge of the available CSI. Since the perfect CSI of the eavesdroppers is also available, we can muddle the eavesdroppers reception more efficiently than the correlation based CSI case in Section V-B. The concept is that, we will design the AN beamformers such that the AN signal is constructive to the IR while destructive to the Eves. As long as some knowledge of the Eves' channels is available at the transmitter, one can do so by pushing the received signal at the IR towards the decision thresholds (green zone in Fig. 2a) while pushing the received signal at the Eves away from the decision thresholds (red zone in Fig. 2b). This makes correct detection more challenging for the Eves and therefore reduces the receive SINR. The benefit is that given secrecy thresholds can be guaranteed with lower transmit power. More importantly, it will be shown in the following optimization schemes that the secrecy constraints are guaranteed on a symbol-by-symbol basis, rather than the conventional statistical guarantees, which are prone to instantaneous outages.

By denoting $\alpha_{\mathrm{R},k}$ and $\alpha_{\mathrm{I},k}$ as the real and imaginary parts of $\tilde{y}_{\mathrm{e},k}\triangleq\mathbf{h}_{\mathrm{e},k}^T\left(\mathbf{b}_\mathrm{d}+\mathbf{z}e^{-j\phi_\mathrm{d}}\right)$, respectively, $\tilde{y}_{\mathrm{e},k}, \forall k$, will lay in the red zone in Fig. 2b if either of the following two constraints is satisfied

$$\phi_{\mathrm{e},k}\leq-\theta\Longrightarrow\frac{-\alpha_{\mathrm{I},k}}{\alpha_{\mathrm{R},k}-\tilde{\Gamma}_{\mathrm{e},k}}\leq\tan\theta, \quad \forall k, \ \text{if} \ \alpha_{\mathrm{I},k}<0, \tag{23a}$$

$$\phi_{\mathrm{e},k}\geq\theta\Longrightarrow\frac{\alpha_{\mathrm{I},k}}{\alpha_{\mathrm{R},k}-\tilde{\Gamma}_{\mathrm{e},k}}\geq\tan\theta, \quad \forall k, \ \text{if} \ \alpha_{\mathrm{I},k}>0. \tag{23b}$$

Since we aim at keeping the eavesdroppers' received signal outside the green (constructive) zone in Fig. 2b, i.e., $\theta\leq\phi_{\mathrm{e},k}\leq-\theta, \forall k$, we have the entire red zone to search the optimal point that minimizes the transmit power. That is, the SINR restriction constraints at the Eves can be represented by the following system of inequalities

$$-\Im\left\{\mathbf{h}_{\mathrm{e},k}^T\left(\mathbf{b}_\mathrm{d}+\mathbf{z}e^{-j\phi_\mathrm{d}}\right)\right\}\leq\left(\Re\left\{\mathbf{h}_{\mathrm{e},k}^T\left(\mathbf{b}_\mathrm{d}+\mathbf{z}e^{-j\phi_\mathrm{d}}\right)\right\}-\sigma_\mathrm{e}\sqrt{\Gamma_{\mathrm{e},k}}\right)\tan\theta, \quad \forall k, \tag{24a}$$

$$\Im\left\{\mathbf{h}_{\mathrm{e},k}^T\left(\mathbf{b}_\mathrm{d}+\mathbf{z}e^{-j\phi_\mathrm{d}}\right)\right\}\geq\left(\Re\left\{\mathbf{h}_{\mathrm{e},k}^T\left(\mathbf{b}_\mathrm{d}+\mathbf{z}e^{-j\phi_\mathrm{d}}\right)\right\}-\sigma_\mathrm{e}\sqrt{\Gamma_{\mathrm{e},k}}\right)\tan\theta, \quad \forall k, \tag{24b}$$

where $\tilde{\Gamma}_{\mathrm{e},k}\triangleq\sigma_\mathrm{e}\sqrt{\Gamma_{\mathrm{e},k}}$. Thus exploiting the knowledge of the interfering signals (AN in this case), the constructive AN-based precoding design problem with secrecy power minimization objective can be formulated as

$$\mathbf{P3}: \quad \min_{\mathbf{b}_\mathrm{d},\mathbf{z}} \ \left\|\mathbf{b}_\mathrm{d}+\mathbf{z}e^{-j\phi_\mathrm{d}}\right\|^2 \tag{25a}$$

$$\text{s.t.} \ \left|\Im\left\{\mathbf{h}_\mathrm{d}^T\left(\mathbf{b}_\mathrm{d}+\mathbf{z}e^{-j\phi_\mathrm{d}}\right)\right\}\right|\leq\left(\Re\left\{\mathbf{h}_\mathrm{d}^T\left(\mathbf{b}_\mathrm{d}+\mathbf{z}e^{-j\phi_\mathrm{d}}\right)\right\}-\sigma_\mathrm{d}\sqrt{\Gamma_\mathrm{d}}\right)\tan\theta, \tag{25b}$$

$$\text{(24a) and (24b) satisfied.} \tag{25c}$$

Problem (25) is a standard second-order cone program, thus can be efficiently solved using interior-point based solvers [37].

Remark: It is important to note that, by the inclusion of the data symbols in **P1**, **P2** and **P3**, the IR's SNR constraint is guaranteed on a symbol-by-sybmol basis, rather than the statistical secrecy of conventional approaches [20]–[23]. In addition, Eves' secrecy constraints in **P3** are also guaranteed during each symbol period. As will be shown in our results, the statistical constraints of conventional formulation $\mathbf{P}-\mathbf{Conv}$ allow a) for the IR's SINR to instantaneously fall below the required threshold, thus leading to an IR outage; b) for the Eves' secrecy SINRs to be instantaneously higher than the statistical constraint, thus jeopardising the secrecy of the useful data. By employing symbol-by-symbol constraints, the proposed approaches avoid this, and guarantee a continuous enforcement of the IR's and Eves' SINRs.

VII. An Efficient Solution for the Secure Constructive Precoding Problem

In this section, we attempt to develop an efficient solver for the secure constructive AN-based precoding design problem. For brevity, here we explore only the most challenging scenario of constructive-destructive AN precoding problem (25). However, the proposed solution can be downscaled to solve other problem formulations as well. Denoting $\mathbf{x}\triangleq\mathbf{b}_\mathrm{d}+\mathbf{z}e^{-j\phi_\mathrm{d}}$ and $\bar{\mathbf{x}}\triangleq\left[\Re\{\mathbf{x}\}^T \ \ \Im\{\mathbf{x}\}^T\right]^T$, the problem (25) can be

rewritten as

$$\min_{\bar{\mathbf{x}}} \quad \|\bar{\mathbf{x}}\|^2 \tag{26a}$$

$$\text{s.t. } \bar{\mathbf{h}}_{\mathrm{d}}^T\bar{\mathbf{x}} + \sigma_{\mathrm{d}}\sqrt{\Gamma_{\mathrm{d}}}\tan\theta \le \bar{\mathbf{h}}_{\mathrm{d}}^T\boldsymbol{\Psi}\bar{\mathbf{x}}\tan\theta, \tag{26b}$$

$$-\bar{\mathbf{h}}_{\mathrm{d}}^T\bar{\mathbf{x}} + \sigma_{\mathrm{d}}\sqrt{\Gamma_{\mathrm{d}}}\tan\theta \le \bar{\mathbf{h}}_{\mathrm{d}}^T\boldsymbol{\Psi}\bar{\mathbf{x}}\tan\theta, \tag{26c}$$

$$\bar{\mathbf{h}}_{\mathrm{e},k}^T\bar{\mathbf{x}} + \sigma_{\mathrm{e}}\sqrt{\Gamma_{\mathrm{e},k}}\tan\theta \ge \bar{\mathbf{h}}_{\mathrm{e},k}^T\boldsymbol{\Psi}\bar{\mathbf{x}}\tan\theta, \quad \forall k, \tag{26d}$$

$$-\bar{\mathbf{h}}_{\mathrm{e},k}^T\bar{\mathbf{x}} + \sigma_{\mathrm{e}}\sqrt{\Gamma_{\mathrm{e},k}}\tan\theta \le \bar{\mathbf{h}}_{\mathrm{e},k}^T\boldsymbol{\Psi}\bar{\mathbf{x}}\tan\theta, \quad \forall k, \tag{26e}$$

where $\bar{\mathbf{h}}_{\mathrm{d}} \triangleq \left[\Im\{\mathbf{h}_{\mathrm{d}}\}^T \;\; \Re\{\mathbf{h}_{\mathrm{d}}\}^T\right]^T$, $\bar{\mathbf{h}}_{\mathrm{e},k} \triangleq \left[\Im\{\mathbf{h}_{\mathrm{e},k}\}^T \;\; \Re\{\mathbf{h}_{\mathrm{e},k}\}^T\right]^T$, and $\boldsymbol{\Psi} \triangleq \begin{bmatrix} \mathbf{0}_{K,K} & -\mathbf{I}_K \\ \mathbf{I}_K & \mathbf{0}_{K,K} \end{bmatrix}$. Now, by defining the following notations

$$\mathbf{A} \triangleq \sec\theta \begin{bmatrix} -\bar{\mathbf{h}}_{\mathrm{d}}^T + \tan\theta\bar{\mathbf{h}}_{\mathrm{d}}^T\boldsymbol{\Psi} \\ \bar{\mathbf{h}}_{\mathrm{d}}^T + \tan\theta\bar{\mathbf{h}}_{\mathrm{d}}^T\boldsymbol{\Psi} \\ -\bar{\mathbf{h}}_{\mathrm{e},1}^T - \tan\theta\bar{\mathbf{h}}_{\mathrm{e},1}^T\boldsymbol{\Psi} \\ \bar{\mathbf{h}}_{\mathrm{e},1}^T + \tan\theta\bar{\mathbf{h}}_{\mathrm{e},1}^T\boldsymbol{\Psi} \\ \vdots \\ -\bar{\mathbf{h}}_{\mathrm{e},K}^T - \tan\theta\bar{\mathbf{h}}_{\mathrm{e},K}^T\boldsymbol{\Psi} \\ \bar{\mathbf{h}}_{\mathrm{e},K}^T + \tan\theta\bar{\mathbf{h}}_{\mathrm{e},K}^T\boldsymbol{\Psi} \end{bmatrix}, \quad \mathbf{c} \triangleq \begin{bmatrix} \sigma_{\mathrm{d}}\sqrt{\Gamma_{\mathrm{d}}} \\ \sigma_{\mathrm{d}}\sqrt{\Gamma_{\mathrm{d}}} \\ -\sigma_{\mathrm{e}}\sqrt{\Gamma_{\mathrm{e},1}} \\ \sigma_{\mathrm{e}}\sqrt{\Gamma_{\mathrm{e},1}} \\ \vdots \\ -\sigma_{\mathrm{e}}\sqrt{\Gamma_{\mathrm{e},K}} \\ \sigma_{\mathrm{e}}\sqrt{\Gamma_{\mathrm{e},K}} \end{bmatrix},$$

we can equivalently rewrite the problem (26) as

$$\min_{\bar{\mathbf{x}}} \quad \|\bar{\mathbf{x}}\|^2 \tag{27a}$$

$$\text{s.t.} \quad -\mathbf{A}\bar{\mathbf{x}} + \mathbf{c} \le \mathbf{0}_{2K+2}, \tag{27b}$$

where $\mathbf{A}$ is a $(2K+2)\times 2N_{\mathrm{T}}$ matrix. The Lagrangian dual function of the problem (27) is given by

$$\mathcal{L}(\bar{\mathbf{x}}, \boldsymbol{\lambda}) \triangleq \|\bar{\mathbf{x}}\|^2 + \boldsymbol{\lambda}^T\left(-\mathbf{A}\bar{\mathbf{x}} + \mathbf{c}\right), \tag{28}$$

where $\boldsymbol{\lambda} \ge \mathbf{0}$ is a $(2K+2)\times 1$ Lagrangian dual variable associated with the constraint (27b). Setting $\frac{\partial\mathcal{L}(\bar{\mathbf{x}},\boldsymbol{\lambda})}{\partial\bar{\mathbf{x}}} = \mathbf{0}_{2K+2}$, we obtain the optimal solution to the problem (27) as

$$\bar{\mathbf{x}}^* = \frac{1}{2}\mathbf{A}^T\boldsymbol{\lambda}. \tag{29}$$

Thus the remaining task to find the optimal $\bar{\mathbf{x}}^*$ is to find the optimal dual variables $\boldsymbol{\lambda}^*$. Substituting $\bar{\mathbf{x}}^*$ into (28), we formulate the dual problem of (27) as

$$\min_{\boldsymbol{\lambda}} \quad f(\boldsymbol{\lambda}) \triangleq \frac{\left\|\mathbf{A}^T\boldsymbol{\lambda}\right\|^2}{4} - \mathbf{c}^T\boldsymbol{\lambda}. \tag{30}$$

In general, it is difficult to derive the optimal solution to the non-negative least-squares problem (30). In the following, we propose a gradient descent algorithm to solve it. Note that the gradient of $f(\boldsymbol{\lambda})$ is given by

$$\nabla f(\boldsymbol{\lambda}) = \frac{\mathbf{A}\mathbf{A}^T\boldsymbol{\lambda}}{2} - \mathbf{c}. \tag{31}$$

Algorithm 1 summarizes the gradient descent method for solving problem (30). Finally, we can obtain the optimal beamforming vectors from $\mathbf{x}^*$ as follows [8]:

$$\mathbf{b}_{\mathrm{d}}^* = \frac{\mathbf{x}^*}{K+1} \tag{32}$$

$$\mathbf{b}_{\mathrm{n},i}^* = \frac{\mathbf{x}^* e^{-j\phi_{\mathrm{d}}}}{K+1}, \forall i. \tag{33}$$

Algorithm 1 Efficient Gradient Descent Algorithm to Solve Problem (30)

1: **Input:** $\mathbf{A}$, $\mathbf{c}$.
2: Initialize $\boldsymbol{\lambda}^{(0)} \ge \mathbf{0}$ and $i = 0$.
3: **repeat**
4: i:= i + 1.
5: Compute the direction of the gradient $\nabla f(\boldsymbol{\lambda}^{(i-1)})$.
6: Choose a_i using backtracking linear search to update $\boldsymbol{\lambda}^{(i)}$:

$$\boldsymbol{\lambda}^{(i)} = \max\left(\boldsymbol{\lambda}^{(i-1)} - a_i\nabla f(\boldsymbol{\lambda}^{(i-1)}), \mathbf{0}_{2K+2}\right).$$

7: **until** convergence.
8: **Output:** Optimal dual variable $\boldsymbol{\lambda}^*$.

VIII. Robust Precoding With Imperfect Full CSI

In the previous sections, secure precoding schemes have been developed assuming partial/statistical/full CSI available at the transmitter. In this section, we consider a secure communication scenario where CSI of all nodes is obtainable through channel training. However, the estimated CSI is imperfect due to quantization and detection errors. Hence we study robust AN precoding design based on that imperfect CSI estimates.

We model the imperfect CSI considering the widely used Gaussian channel error model such that the channel error vectors have circularly symmetric complex Gaussian (CSCG) distribution. Thus, the actual channels between the BS and the IR can be modeled as

$$\mathbf{h}_{\mathrm{d}} = \hat{\mathbf{h}}_{\mathrm{d}} + \mathbf{e}_{\mathrm{d}}, \tag{34}$$

and that between the BS and the kth Eve can be modelled as

$$\mathbf{h}_{\mathrm{e},k} = \hat{\mathbf{h}}_{\mathrm{e},k} + \mathbf{e}_{\mathrm{e},k}, \forall k, \tag{35}$$

where $\hat{\mathbf{h}}_{\mathrm{d}}$ and $\hat{\mathbf{h}}_{\mathrm{e},k}, \forall k$, denote the imperfect estimated CSI available at the BS and $\mathbf{e}_{\mathrm{d}}$, $\mathbf{e}_{\mathrm{e},k} \in \mathbb{C}^{N_{\mathrm{T}}\times 1}, \forall k$, represent the channel uncertainties such that $\|\mathbf{e}_{\mathrm{d}}\|^2 \le \varepsilon_{\mathrm{d}}^2$, and $\|\mathbf{e}_{\mathrm{e},k}\|^2 \le \varepsilon_{\mathrm{e}}^2, \forall k$, respectively.

A. Conventional AN-Aided Robust Secure Precoding

Conventional AN-aided downlink robust secrecy power minimization problem with SINR constraints is formulated as

$$\min_{\mathbf{b}_{\mathrm{d}},\mathbf{z}} \quad \|\mathbf{b}_{\mathrm{d}}\|^2 + \|\mathbf{z}\|^2 \tag{36a}$$

$$\text{s.t.} \quad \min_{\|\mathbf{e}_{\mathrm{d}}\|\le\varepsilon_{\mathrm{d}}} \frac{\left|\mathbf{h}_{\mathrm{d}}^T\mathbf{b}_{\mathrm{d}}\right|^2}{\left|\mathbf{h}_{\mathrm{d}}^T\mathbf{z}\right|^2 + \sigma_{\mathrm{d}}^2} \ge \Gamma_{\mathrm{d}}, \tag{36b}$$

$$\max_{\|\mathbf{e}_{\mathrm{e},k}\|\le\varepsilon_{\mathrm{e}}} \frac{\left|\mathbf{h}_{\mathrm{e},k}^T\mathbf{b}_{\mathrm{d}}\right|^2}{\left|\mathbf{h}_{\mathrm{e},k}^T\mathbf{z}\right|^2 + \sigma_{\mathrm{e}}^2} \le \Gamma_{\mathrm{e},k}, \quad \forall k. \tag{36c}$$

Due to the spherical channel uncertainty model, constraints (36b) and (36c) actually involve infinitely many constraints which makes the problem (36) very difficult to solve. However, applying $\mathcal{S}$-procedure [22, Lemma 2], the inequality constraints in (36) can be transformed into convex LMI constraints and thus problem (36) can be readily solved using existing

$$\min_{\mathbf{b}_\mathrm{d},\mathbf{z}} \quad \left\|\mathbf{b}_\mathrm{d}+\mathbf{z}e^{-j\phi_\mathrm{d}}\right\|^2 \tag{37a}$$

$$\text{s.t.} \quad \left|\Im\left\{\mathbf{h}_\mathrm{d}^T\left(\mathbf{b}_\mathrm{d}+\mathbf{z}e^{-j\phi_\mathrm{d}}\right)\right\}\right| \le \left(\Re\left\{\mathbf{h}_\mathrm{d}^T\left(\mathbf{b}_\mathrm{d}+\mathbf{z}e^{-j\phi_\mathrm{d}}\right)\right\}-\sigma_\mathrm{d}\sqrt{\Gamma_\mathrm{d}}\right)\tan\theta, \forall\|\mathbf{e}_\mathrm{d}\|\le\varepsilon_\mathrm{d}, \tag{37b}$$

$$-\Im\left\{\mathbf{h}_{\mathrm{e},k}^T\left(\mathbf{b}_\mathrm{d}+\mathbf{z}e^{-j\phi_\mathrm{d}}\right)\right\} \le \left(\Re\left\{\mathbf{h}_{\mathrm{e},k}^T\left(\mathbf{b}_\mathrm{d}+\mathbf{z}e^{-j\phi_\mathrm{d}}\right)\right\}-\sigma_\mathrm{e}\sqrt{\Gamma_{\mathrm{e},k}}\right)\tan\theta, \forall\|\mathbf{e}_{\mathrm{e},k}\|\le\varepsilon_\mathrm{e}, \forall k, \tag{37c}$$

$$\Im\left\{\mathbf{h}_{\mathrm{e},k}^T\left(\mathbf{b}_\mathrm{d}+\mathbf{z}e^{-j\phi_\mathrm{d}}\right)\right\} \ge \left(\Re\left\{\mathbf{h}_{\mathrm{e},k}^T\left(\mathbf{b}_\mathrm{d}+\mathbf{z}e^{-j\phi_\mathrm{d}}\right)\right\}-\sigma_\mathrm{e}\sqrt{\Gamma_{\mathrm{e},k}}\right)\tan\theta, \forall\|\mathbf{e}_{\mathrm{e},k}\|\le\varepsilon_\mathrm{e}, \forall k. \tag{37d}$$

solvers. It has been proved in [23] that whenever problem (36) is feasible, the corresponding transmit precoding solution is of rank-one hence optimal.

B. Constructive AN-Aided Robust Secure Precoding

In this section, we aim at constructive AN based robust secure precoding design with imperfect knowledge of all CSI, as opposed to its perfect CSI counterpart in Section VI. With the deterministic channel uncertainty model described above, we consider worst-case based robust design. Thus the constructive AN based robust power minimization problem can be formulated as given in (37) (at the top of the this page).

Note that the information and the AN beamforming vectors appear in identical form in the objective functions as well as in the constraints in problem (37). Denoting $\mathbf{b}\triangleq\mathbf{b}_\mathrm{d}+\mathbf{z}e^{-j\phi_\mathrm{d}}$, the problem can thus be represented as

$$\min_{\mathbf{b}_\mathrm{d},\mathbf{z}} \quad \|\mathbf{b}\|^2 \tag{38a}$$

$$\text{s.t.} \quad \left|\Im\left\{\left(\hat{\mathbf{h}}_\mathrm{d}+\mathbf{e}_\mathrm{d}\right)^T\mathbf{b}\right\}\right| \le \left(\Re\left\{\left(\hat{\mathbf{h}}_\mathrm{d}+\mathbf{e}_\mathrm{d}\right)^T\mathbf{b}\right\} -\sigma_\mathrm{d}\sqrt{\Gamma_\mathrm{d}}\right)\tan\theta, \quad \forall\|\mathbf{e}_\mathrm{d}\|\le\varepsilon_\mathrm{d}, \tag{38b}$$

$$-\Im\left\{\left(\hat{\mathbf{h}}_{\mathrm{e},k}+\mathbf{e}_{\mathrm{e},k}\right)^T\mathbf{b}\right\} \le \left(\Re\left\{\left(\hat{\mathbf{h}}_{\mathrm{e},k}+\mathbf{e}_{\mathrm{e},k}\right)^T \times\mathbf{b}\right\}-\sigma_\mathrm{e}\sqrt{\Gamma_{\mathrm{e},k}}\right)\tan\theta, \quad \forall\|\mathbf{e}_{\mathrm{e},k}\|\le\varepsilon_\mathrm{e}, \quad \forall k, \tag{38c}$$

$$\Im\left\{\left(\hat{\mathbf{h}}_{\mathrm{e},k}+\mathbf{e}_{\mathrm{e},k}\right)^T\mathbf{b}\right\} \ge \left(\Re\left\{\left(\hat{\mathbf{h}}_{\mathrm{e},k}+\mathbf{e}_{\mathrm{e},k}\right)^T\mathbf{b}\right\} -\sigma_\mathrm{e}\sqrt{\Gamma_{\mathrm{e},k}}\right)\tan\theta, \quad \forall\|\mathbf{e}_{\mathrm{e},k}\|\le\varepsilon_\mathrm{e}, \ \forall k. \tag{38d}$$

Considering the real and imaginary parts of each complex vector separately, we have

$$\mathbf{h}_\mathrm{d}=\hat{\mathbf{h}}_{R,\mathrm{d}}+j\hat{\mathbf{h}}_{I,\mathrm{d}}+\mathbf{e}_{R,\mathrm{d}}+j\mathbf{e}_{I,\mathrm{d}}, \tag{39}$$

$$\mathbf{b}=\mathbf{b}_R+j\mathbf{b}_I, \tag{40}$$

where the subscripts R and I indicate the real and imaginary components of the corresponding complex notation, respectively. As such, we have the real part,

$$\begin{aligned}\Re\left\{\left(\hat{\mathbf{h}}_\mathrm{d}+\mathbf{e}_\mathrm{d}\right)^T\mathbf{b}\right\} &= \hat{\mathbf{h}}_{R,\mathrm{d}}^T\mathbf{b}_R-\hat{\mathbf{h}}_{I,\mathrm{d}}^T\mathbf{b}_I+\mathbf{e}_{R,\mathrm{d}}^T\mathbf{b}_R-\mathbf{e}_{I,\mathrm{d}}^T\mathbf{b}_I\\ &= \tilde{\mathbf{h}}_\mathrm{d}^T\mathbf{b}_1+\tilde{\mathbf{e}}_\mathrm{d}^T\mathbf{b}_1,\end{aligned} \tag{41}$$

where $\tilde{\mathbf{h}}_\mathrm{d}\triangleq\left[\hat{\mathbf{h}}_{R,\mathrm{d}}^T \ \ \hat{\mathbf{h}}_{I,\mathrm{d}}^T\right]^T$, $\tilde{\mathbf{e}}_\mathrm{d}\triangleq\left[\mathbf{e}_{R,\mathrm{d}}^T \ \ \mathbf{e}_{I,\mathrm{d}}^T\right]^T$, and $\mathbf{b}_1\triangleq\left[\mathbf{b}_R^T \ \ -\mathbf{b}_I^T\right]^T$. Similarly, the imaginary component can be expressed as

$$\begin{aligned}\Im\left\{\left(\hat{\mathbf{h}}_\mathrm{d}+\mathbf{e}_\mathrm{d}\right)^T\mathbf{b}\right\} &= \hat{\mathbf{h}}_{R,\mathrm{d}}^T\mathbf{b}_R+\hat{\mathbf{h}}_{I,\mathrm{d}}^T\mathbf{b}_I+\mathbf{e}_{R,\mathrm{d}}^T\mathbf{b}_R+\mathbf{e}_{I,\mathrm{d}}^T\mathbf{b}_I\\ &= \tilde{\mathbf{h}}_\mathrm{d}^T\mathbf{b}_2+\tilde{\mathbf{e}}_\mathrm{d}^T\mathbf{b}_2,\end{aligned} \tag{42}$$

with $\mathbf{b}_2\triangleq\left[\mathbf{b}_R^T \ \ \mathbf{b}_I^T\right]^T$. Thus the constraint (38b) can be explicitly expressed as the following two constraints

$$\max_{\|\mathbf{e}_\mathrm{d}\|\le\varepsilon_\mathrm{d}} \ \tilde{\mathbf{h}}_\mathrm{d}^T\mathbf{b}_2+\tilde{\mathbf{e}}_\mathrm{d}^T\mathbf{b}_2-\left(\tilde{\mathbf{h}}_\mathrm{d}^T\mathbf{b}_1+\tilde{\mathbf{e}}_\mathrm{d}^T\mathbf{b}_1\right)\tan\theta +\sigma_\mathrm{d}\sqrt{\Gamma_\mathrm{d}}\tan\theta\le 0 \tag{43}$$

$$\max_{\|\mathbf{e}_\mathrm{d}\|\le\varepsilon_\mathrm{d}} \ -\tilde{\mathbf{h}}_\mathrm{d}^T\mathbf{b}_2-\tilde{\mathbf{e}}_\mathrm{d}^T\mathbf{b}_2-\left(\tilde{\mathbf{h}}_\mathrm{d}^T\mathbf{b}_1+\tilde{\mathbf{e}}_\mathrm{d}^T\mathbf{b}_1\right)\tan\theta +\sigma_\mathrm{d}\sqrt{\Gamma_\mathrm{d}}\tan\theta\le 0. \tag{44}$$

Similarly, the constraints (38c) and (38d) can be, respectively, rewritten as

$$\max_{\|\mathbf{e}_{\mathrm{e},k}\|\le\varepsilon_\mathrm{e}} \ -\tilde{\mathbf{h}}_{\mathrm{e},k}^T\mathbf{b}_2-\tilde{\mathbf{e}}_{\mathrm{e},k}^T\mathbf{b}_2-\left(\tilde{\mathbf{h}}_{\mathrm{e},k}^T\mathbf{b}_1+\tilde{\mathbf{e}}_{\mathrm{e},k}^T\mathbf{b}_1\right)\tan\theta +\sigma_\mathrm{e}\sqrt{\Gamma_{\mathrm{e},k}}\tan\theta\le 0 \tag{45}$$

$$\min_{\|\mathbf{e}_{\mathrm{e},k}\|\le\varepsilon_\mathrm{e}} \ \tilde{\mathbf{h}}_{\mathrm{e},k}^T\mathbf{b}_2+\tilde{\mathbf{e}}_{\mathrm{e},k}^T\mathbf{b}_2-\left(\tilde{\mathbf{h}}_{\mathrm{e},k}^T\mathbf{b}_1+\tilde{\mathbf{e}}_{\mathrm{e},k}^T\mathbf{b}_1\right)\tan\theta +\sigma_\mathrm{e}\sqrt{\Gamma_{\mathrm{e},k}}\tan\theta\ge 0, \tag{46}$$

where $\tilde{\mathbf{h}}_{\mathrm{e},k}\triangleq\left[\mathbf{h}_{R\mathrm{e},k}^T \ \ \mathbf{h}_{I\mathrm{e},k}^T\right]^T$. By replacing the CSI error bounds in these constraints, the robust problem (38) can be reformulated as

$$\min_{\mathbf{b}_1,\mathbf{b}_2} \ \|\mathbf{b}_2\|^2 \quad \text{s.t.} \tag{47a}$$

$$\tilde{\mathbf{h}}_\mathrm{d}^T\mathbf{b}_2-\tilde{\mathbf{h}}_\mathrm{d}^T\mathbf{b}_1\tan\theta+\varepsilon_\mathrm{d}\|\mathbf{b}_2-\mathbf{b}_1\tan\theta\| +\sigma_\mathrm{d}\sqrt{\Gamma_\mathrm{d}}\le 0 \tag{47b}$$

$$-\tilde{\mathbf{h}}_\mathrm{d}^T\mathbf{b}_2-\tilde{\mathbf{h}}_\mathrm{d}^T\mathbf{b}_1\tan\theta+\varepsilon_\mathrm{d}\|\mathbf{b}_2+\mathbf{b}_1\tan\theta\| +\sigma_\mathrm{d}\sqrt{\Gamma_\mathrm{d}}\le 0, \tag{47c}$$

$$-\tilde{\mathbf{h}}_{\mathrm{e},k}^T\mathbf{b}_2-\tilde{\mathbf{h}}_{\mathrm{e},k}^T\mathbf{b}_1\tan\theta-\varepsilon_\mathrm{e}\|\mathbf{b}_2+\mathbf{b}_1\|\tan\theta +\sigma_\mathrm{e}\sqrt{\Gamma_{\mathrm{e},k}}\le 0 \tag{47d}$$

$$\tilde{\mathbf{h}}_{\mathrm{e},k}^T\mathbf{b}_2+\tilde{\mathbf{h}}_{\mathrm{e},k}^T\mathbf{b}_1\tan\theta-\varepsilon_\mathrm{e}\|\mathbf{b}_2+\mathbf{b}_1\|\tan\theta +\sigma_\mathrm{e}\sqrt{\Gamma_{\mathrm{e},k}}\ge 0. \tag{47e}$$

The SOCP problem (47) can be efficiently solved using existing solvers [37].

Finally, we analyze the computational complexity of the problems **P1**, **P2** and **P3** based on interior-point method based solvers. Note that in all three formulations, the number of decision variables is on the order of $2N_\mathrm{T}$. Let us first examine problem **P1**, which has 2 LMI constraints of size 1 (due to

TABLE I

COMPLEXITY ANALYSIS OF THE PROPOSED APPROACHES

Problem	Complexity Order ($n = \mathcal{O}(2N_{\mathrm{T}})$)
P1	$\ln(1/\epsilon)2n(N_{\mathrm{T}}^2+n^2+2n+2)$
P2	$\ln(1/\epsilon)\sqrt{(2K+2)}n(n^2+2n+2)$
P3	$\ln(1/\epsilon)2n(n^2+4n+4)$
Robust problem (47)	$\ln(1/\epsilon)\sqrt{8}n(64N_{\mathrm{T}}^2+n^2)$

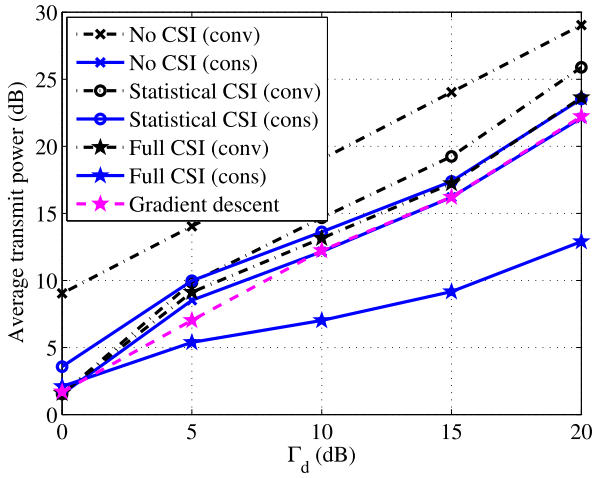

Fig. 3. Transmit power P_{T} versus required SINR at IR Γ_{d} with $N_{\mathrm{T}} = 6$, $K = 3$, and $\Gamma_{\mathrm{e}} = -5$ (dB).

the $|\cdot|$ operation) and 1 SOC constraint of size N_{T}. Thus the complexity of problem **P1** is on the order shown in the first row of Table I [25], [38]. Similarly, the complexity of problem **P2** and problem **P3** can be quantified as shown in the second and the third row of Table I, respectively. The complexity of the robust problem (47) is shown in the last row.

IX. SIMULATION RESULTS

This section presents numerical simulation results to evaluate the performance of the proposed constructive interference based PLS algorithms in a MISO wiretap channel. For comparison, conventional secure precoding performances have also been included. For simplicity, it was assumed that $\Gamma_{\mathrm{e},k} = \Gamma_{\mathrm{e}}$, $\forall k$ and $\sigma_{\mathrm{d}}^2 = \sigma_{\mathrm{e}}^2 = 1$. Unless otherwise specified, $N = 3$ and QPSK is the modulation scheme considered, while it has been shown that the concept of constructive interference also offers benefits to larger scale systems and higher order PSK and QAM modulations [3], [39]. All the estimated channel vectors are generated as independent and identically distributed complex Gaussian random variables with mean zero and the TGn path-loss model for urban cellular environment is adopted considering a path-loss exponent of 2.7 [40]. All simulation results are averaged over 1000 independent channel realizations, unless explicitly mentioned. In the following simulations, we compare the performance of the proposed approaches with that of the conventional AN-aided precoding scheme in [31] as the benchmark.

We start the performance evaluation of the proposed constructive interference based secure AN precoding schemes with varying extent of CSI of the eavesdropping nodes available at the transmitter. Fig. 3 shows the average transmit power required versus the SINR requirement at the IR for the no Eves' CSI case (Section IV), the statistical Eves' CSI case (Section V), the full CSI case (Section VI), and the gradient descent method (Algorithm 1), as compared with the corresponding conventional AN precoding schemes for $N_{\mathrm{T}} = 6$, $K = 3$, and $\Gamma_{\mathrm{e}} = -5$ (dB). For a fairer comparison, we set $P_t = \frac{N_{\mathrm{T}}\Gamma_{\mathrm{d}}}{\sigma_{\mathrm{d}}^2}$ for the isotropic AN design with $\rho = \frac{1}{2}$. It can be observed that the proposed constructive interference algorithms achieve significant power gains compared to the conventional AN precoding schemes. Interestingly, the constructive isotropic AN scheme (No CSI) requires lower power compared to the statistical CSI counterpart, which is due to the fact that the isotropic AN scheme does not impose eavesdropping constraints. However, the superiority of the statistical CSI algorithm remains in the secrecy guarantee, which we will observe in the next example. Note that although the gradient descent algorithm requires higher power compared to the constructive AN schemes, it requires much lower execution time yet satisfying the instantaneous SINR constraints [8], which we will observe in Figs. 5 and 6.

Next, we demonstrate the effects of the different extent of available Eves' CSI on the resulting Eve's SINR. The histograms of the instantaneously obtained SINRs at the Eves normalized by the eavesdropping threshold Γ_{e} with $N_{\mathrm{T}} = 6$, $K = 4$, for different CSI cases have been plotted in Fig. 4. The red lines at position 1 indicate the normalized threshold value of the corresponding constraint. It can be observed that in many cases the instantaneous secrecy thresholds are not satisfied under the conventional average Eves' SINR constraints, which jeopardizes the information secrecy. For the constructive precoding schemes with no Eve's CSI, in line with the conventional precoding, no secrecy can be guaranteed since there is no explicit secrecy constraint. However, the statistical Eves' CSI significantly improves secrecy guarantee. The Eves' SINR is perfectly constrained only with full CSI of all nodes. These results demonstrate the importance of CSI accuracy for improving information secrecy.

Fig. 5 shows the average execution time of the algorithms per optimization versus the number of Eves for the full and perfect CSI case only, with $N_{\mathrm{T}} = 6$, $\Gamma_{\mathrm{d}} = 10$ (dB), and $\Gamma_{\mathrm{e}} = -5$ (dB). Specifically, we denote the conventional precoding schemes as 'Conv Prec', the constructive interference based precoding scheme developed in Section VI-B as 'Const Prec' with conventional eavesdropping constraints, and the destructive interference based scheme in the same section as 'Const-Dest Prec' in the figures below. The gradient descent algorithm is denoted as 'Gradient Desc'. Note that the conventional approach requires the highest time while the gradient descent approach takes the lowest time. However, the 'Const Prec' and the 'Const-Dest Prec' algorithms require almost identical time to execute. Next, for a fairer comparison and noting that the proposed optimizations need to be solved on a symbol basis, we analyze the average execution time per frame considering the LTE Type 2 downlink TDD frame structure defined in [41]. In a Type 2 downlink TDD frame, 5 out of the 10 sub-frames are designated for downlink

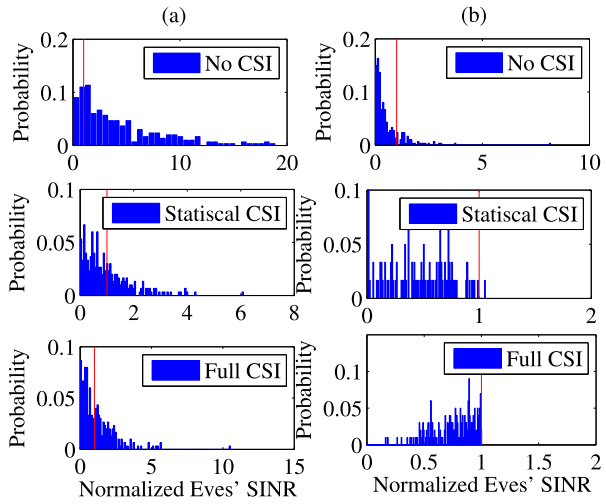

Fig. 4. Histogram of the average Eves' SINR normalized by the threshold Γ_e with $N_T = 6$, $K = 4$. (a) Conventional precoding. (b) Constructive precoding.

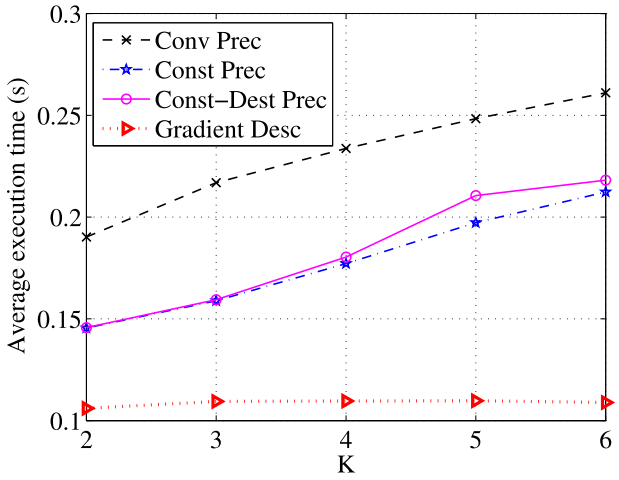

Fig. 5. Average execution time (seconds) versus K with $N_T = 6$, $\Gamma_d = 10$ (dB), and $\Gamma_e = -5$ (dB).

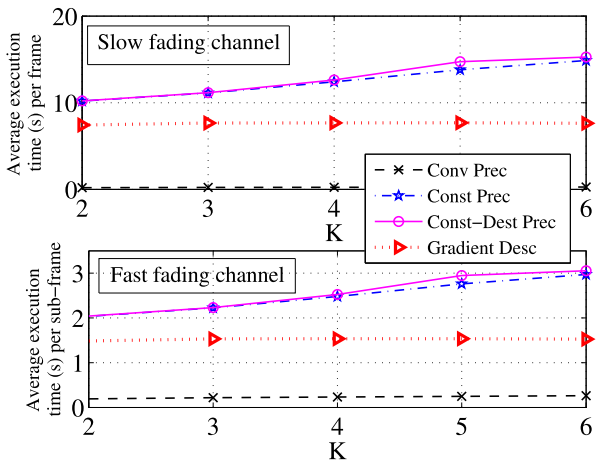

Fig. 6. Average execution time (s) versus K for slow/fast fading channels with $N_T = 6$, $\Gamma_d = 10$ (dB), and $\Gamma_e = -5$ (dB).

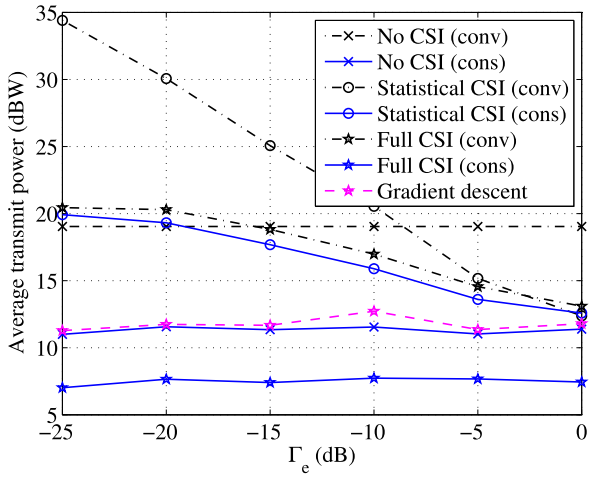

Fig. 7. Transmit power P_T versus required SINR Γ_e with $N_T = 6$, $K = 4$, and $\Gamma_d = 10$ (dB).

transmission, each containing 14 symbols. Therefore, the downlink adopts a block size of 70. We consider two cases; a slow fading case where the channel remains constant for the whole duration of the frame, and a fast fading case where the channel is constant only for a signle sub-frame. In a typical slow fading environment, channel coefficients are assumed to be constant over one frame duration and hence updated only once. Thus the conventional precoding scheme executes only once over a frame duration. However, the proposed symbol-by-symbol precoding schemes need to execute 70 times over one frame period. For the fast fading case, the CSI and hence the conventional optimization is updated 5 times per frame. It can be seen from Fig. 6 that, while higher than that of the conventional schemes, the per-frame complexity of the proposed approaches is still comparable. The significant performance gains offered by our approaches therefore make their performance-complexity trade-off favourable.

In the next example, we examine the transmit power requirement against the maximum allowable eavesdropping SINR Γ_e assuming perfect CSI of all nodes. Fig. 7 plots the average transmit power P_T versus Γ_e for $N_T = 6$, $K = 4$ and $\Gamma_d = 10(dB)$. The results in Fig. 7 are consistent with those in Fig. 3 in the sense that the proposed constructive interference precoding schemes yield the best performance. Note that the required transmit power for the isotropic beamforming schemes (No CSI) are invariant of the Eves' SINR threshold since they do not consider blocking the eavesdroppers. However, for the other schemes, with the increase in the allowable SINR threshold at the Eves, the required transmit power gradually decreases due to the relaxed eavesdropping constraints. In any case, the constructive interference based precoding schemes outperform the conventional AN-aided secure precoding scheme.

Next, we demonstrate the effects of the constructive and destructive AN on the IR's as well as the Eves' SINR constraints. The histograms of the instantaneously obtained SINRs at the IR and Eves normalized by the corresponding thresholds (i.e., Γ_d for the IR and Γ_e for the Eves) with $N_T = 6$, $K = 4$, for different schemes have been plotted in Fig. 8. The red lines at position 1 indicate the normalized threshold value of the corresponding constraints. It can be observed that in many cases the instantaneous SINR thresholds are not satisfied under

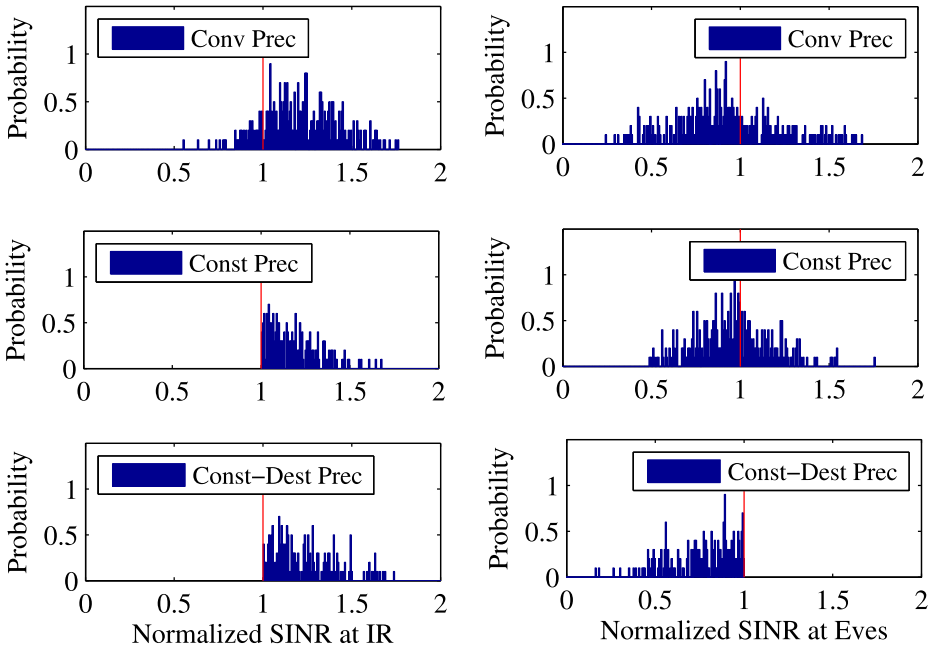

Fig. 8. Normalized histogram of the average SINR with $N_T = 6, K = 4$.

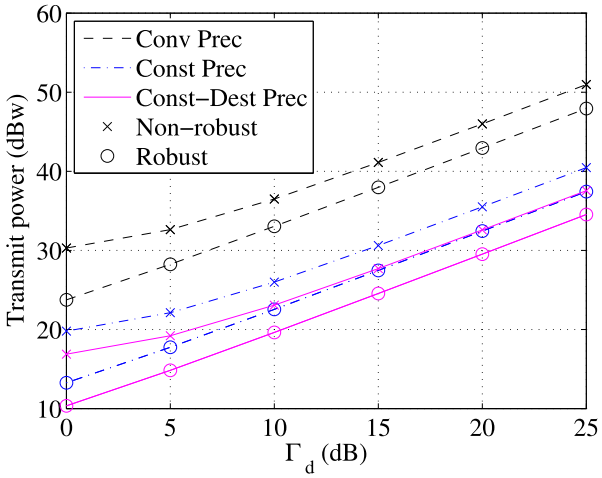

Fig. 9. Transmit power P_T versus required SINR Γ_d with $N_T = 6, K = 3$, $\Gamma_e = -5$ (dB), and $\varepsilon_d = 0.1, \varepsilon_e = 0.3$ (dB).

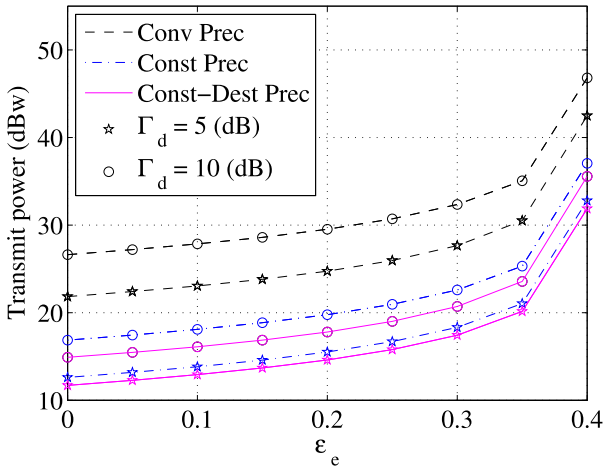

Fig. 10. Transmit power P_T versus Eves' CSI error bound ε_e with $N_T = 6, K = 3$, $\varepsilon_d = 0.1$, $\Gamma_e = -5$ (dB), and $\Gamma_d = 5$ (dB), 10 (dB).

the conventional average SINR constraints for both the IR and the Eves. Indeed, the IR has instantaneous SINRs that are below the threshold requirements, which would lead to SINR outages. More importantly, the Eves' receive instantaneous SINR above the secrecy threshold jeopardizes the information secrecy. However, the SINR threshold is always satisfied for the IR under the constructive AN schemes, although the Eves' SINR is perfectly constrained only under the 'Const-Dest Prec' scheme. These results demonstrate significant gain in terms of information secrecy by the proposed schemes.

Finally, we turn our attention to the imperfect CSI case (Section VIII), where we analyze the performance of the proposed robust beamforming designs in Figs. 9 and 10 with $N_T = 6, K = 3, \Gamma_e = -5$ (dB). In Fig. 9, the robust schemes indicate the solutions to the problems (36) and (47), respectively, for conventional and constructive precoding schemes for $\varepsilon_d = 0.1, \varepsilon_e = 0.3$. On the other hand, the 'Non-robust' scheme is designed treating the imperfect channel estimates available at the BS as the perfect CSI, hence yields noticeable performance degradation. However, the proposed constructive interference based robust secure beamforming schemes demonstrate significant transmit power gains. Fig. 10 shows the required transmit power of the robust algorithms across a wide range of Eves' CSI uncertainty with $N_T = 6, K = 3$, $\varepsilon_d = 0.1$, $\Gamma_e = -5$ (dB), and $\Gamma_d = 5$ (dB), 10 (dB). It can be observed that as the CSI error bound increases (i.e., with lower extent of CSI available at the transmitter), the required transmit power significantly increases in order to satisfy the SINR requirements.

X. Conclusions

We proposed the novel idea of designing the AN-aided secure precoding schemes as constructive to the IR and

destructive to the Eves. This introduces a major breakthrough in the conventional approach of transmitting AN for improving PLS. The concept opens up new opportunities for expanding the secrecy rate regions. We studied the downlink transmit power minimization problem considering both perfect and imperfect CSI at the BS. Simulation results demonstrated that significant performance gain is achievable by the proposed constructive AN precoding schemes compared to the conventional schemes and have established the proposed approach as a new dimension in the design of PLS.

REFERENCES

[1] M. R. A. Khandaker and Y. Rong, "Interference MIMO relay channel: Joint power control and transceiver-relay beamforming," *IEEE Trans. Signal Process.*, vol. 60, no. 12, pp. 6509–6518, Dec. 2012.

[2] M. R. A. Khandaker and K.-K. Wong, "Joint source and relay optimization for interference MIMO relay networks," *EURASIP J. Adv. Signal Process.*, vol. 24, p. 24, Dec. 2017.

[3] C. Masouros, T. Ratnarajah, M. Sellathurai, C. B. Papadias, and A. K. Shukla, "Known interference in the cellular downlink: A performance limiting factor or a source of green signal power?" *IEEE Commun. Mag.*, vol. 51, no. 10, pp. 162–171, Oct. 2013.

[4] G. Zheng, I. Krikidis, C. Masouros, S. Timotheou, D.-A. Toumpakaris, and Z. Ding, "Rethinking the role of interference in wireless networks," *IEEE Commun. Mag.*, vol. 52, no. 11, pp. 152–158, Nov. 2014.

[5] C. Masouros and E. Alsusa, "Dynamic linear precoding for the exploitation of known interference in MIMO broadcast systems," *IEEE Trans. Wireless Commun.*, vol. 8, no. 3, pp. 1396–1404, Mar. 2009.

[6] C. Masouros, "Correlation rotation linear precoding for MIMO broadcast communications," *IEEE Trans. Signal Process.*, vol. 59, no. 1, pp. 252–262, Jan. 2011.

[7] C. Masouros, M. Sellathurai, and T. Ratnarajah, "Vector perturbation based on symbol scaling for limited feedback MISO downlinks," *IEEE Trans. Signal Process.*, vol. 62, no. 3, pp. 562–571, Feb. 2014.

[8] C. Masouros and G. Zheng, "Exploiting known interference as green signal power for downlink beamforming optimization," *IEEE Trans. Signal Process.*, vol. 63, no. 14, pp. 3628–3640, Jul. 2015.

[9] E. Alsusa and C. Masouros, "Adaptive code allocation for interference management on the downlink of DS-CDMA systems," *IEEE Trans. Wireless Commun.*, vol. 7, no. 7, pp. 2420–2424, Jul. 2008.

[10] M. Alodeh, S. Chatzinotas, and B. Ottersten, "Constructive multiuser interference in symbol level precoding for the MISO downlink channel," *IEEE Trans. Signal Process.*, vol. 63, no. 9, pp. 2239–2252, May 2015.

[11] S. Timotheou, G. Zheng, C. Masouros, and I. Krikidis, "Exploiting constructive interference for simultaneous wireless information and power transfer in multiuser downlink systems," *IEEE J. Sel. Areas Commun.*, vol. 34, no. 5, pp. 1772–1784, May 2016.

[12] A. Li and C. Masouros, "Exploiting constructive mutual coupling in P2P MIMO by analog-digital phase alignment," *IEEE Trans. Wireless Commun.*, vol. 16, no. 3, pp. 1948–1962, Mar. 2017.

[13] K. L. Law, C. Masouros, and M. Pesavento, "Transmit precoding for interference exploitation in the underlay cognitive radio Z-channel," *IEEE Trans. Signal Process.*, vol. 65, no. 14, pp. 3617–3631, Jul. 2017.

[14] P. V. Amadori and C. Masouros, "Interference-driven antenna selection for massive multiuser MIMO," *IEEE Trans. Veh. Technol.*, vol. 65, no. 8, pp. 5944–5958, Aug. 2016.

[15] P. V. Amadori and C. Masouros, "Constant envelope precoding by interference exploitation in phase shift keying-modulated multiuser transmission," *IEEE Trans. Wireless Commun.*, vol. 16, no. 1, pp. 538–550, Jan. 2017.

[16] P. V. Amadori and C. Masouros, "Large scale antenna selection and precoding for interference exploitation," *IEEE Trans. Commun.*, vol. 65, no. 10, pp. 4529–4542, Oct. 2017.

[17] A. Li, C. Masouros, F. Liu, and L. Swindlehurst, "Massive MIMO 1-bit DAC transmission: A low-complexity symbol scaling approach," *IEEE Trans. Wireless Commun.*, to be published.

[18] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.

[19] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 3, pp. 339–348, May 1978.

[20] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.

[21] Q. Li and W.-K. Ma, "Spatially selective artificial-noise aided transmit optimization for MISO multi-eves secrecy rate maximization," *IEEE Trans. Signal Process.*, vol. 61, no. 10, pp. 2704–2717, May 2013.

[22] M. R. A. Khandaker and K.-K. Wong, "Masked beamforming in the presence of energy-harvesting eavesdroppers," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 1, pp. 40–54, Jan. 2015.

[23] M. R. A. Khandaker and K.-K. Wong, "Robust secrecy beamforming with energy-harvesting eavesdroppers," *IEEE Wireless Commun. Lett.*, vol. 4, no. 1, pp. 10–13, Feb. 2015.

[24] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1550–1573, 3rd Quart., 2014.

[25] M. R. A. Khandaker, K.-K. Wong, Y. Zhang, and Z. Zheng, "Probabilistically robust SWIPT for secrecy MISOME systems," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 1, pp. 211–226, Jan. 2017.

[26] M. P. Daly and J. T. Bernhard, "Directional modulation technique for phased arrays," *IEEE Trans. Antennas Propag.*, vol. 57, no. 9, pp. 2633–2640, Sep. 2009.

[27] M. P. Daly, E. L. Daly, and J. T. Bernhard, "Demonstration of directional modulation using a phased array," *IEEE Trans. Antennas Propag.*, vol. 58, no. 5, pp. 1545–1550, May 2010.

[28] A. Kalantari, M. Soltanalian, S. Maleki, S. Chatzinotas, and B. Ottersten, "Secure M-PSK communication via directional modulation," in *Proc. IEEE ICASSP*, Shanghai, China, Mar. 2016, pp. 3481–3485.

[29] A. Kalantari, M. Soltanalian, S. Maleki, S. Chatzinotas, and B. Ottersten, "Directional modulation via symbol-level precoding: A way to enhance security," *IEEE J. Sel. Topics Signal Process.*, vol. 10, no. 8, pp. 1478–1493, Dec. 2016. [Online]. Available: http://arXiv:1606.04488v2

[30] M. R. A. Khandaker, C. Masouros, and K.-K. Wong, "Constructive interference based secure precoding," in *Proc. IEEE ISIT*, Aachen, Germany, Jun. 2017, pp. 2875–2879.

[31] W.-C. Liao, T.-H. Chang, W.-K. Ma, and C.-Y. Chi, "QoS-based transmit beamforming in the presence of eavesdroppers: An optimized artificial-noise-aided approach," *IEEE Trans. Signal Process.*, vol. 59, no. 3, pp. 1202–1216, Mar. 2011.

[32] C. Masouros and E. Alsusa, "Two-stage transmitter precoding based on data-driven code-hopping and partial zero forcing beamforming for Mc-CDMA communications," *IEEE Trans. Wireless Commun.*, vol. 8, no. 7, pp. 3634–3645, Jul. 2009.

[33] C. Masouros and E. Alsusa, "Interference exploitation using adaptive code allocation for the downlink of precoded multiple carrier code division multiple access systems," *IET J. Commun.*, vol. 9, no. 9, pp. 1118–1130, Oct. 2008.

[34] C. Masouros and E. Alsusa, "A novel transmitter-based selective-precoding technique for DS/CDMA systems," *IEEE Signal Process. Lett.*, vol. 14, no. 9, pp. 637–640, Sep. 2007.

[35] A. L. Swindlehurst, "Fixed SINR solutions for the MIMO wire-tap channel," in *Proc. IEEE ICASSP*, Taipei, Taiwan, Apr. 2009, pp. 2437–2440.

[36] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, U.K.: Cambridge Univ. Press, 2004.

[37] M. Grant and S. Boyd. (Apr. 2010). *CVX: MATLAB Software for Disciplined Convex Programming (Web Page and Software)*. [Online]. Available: http://cvxr.com/cvx

[38] A. Ben-Tal and A. Nemirovski, *Lectures on Modern Convex Optimization: Analysis, Algorithms, and Engineering Applications* (MPS SIAM Series on Optimization). Philadelphia, PA, USA: SIAM, 2001.

[39] M. Alodeh, S. Chatzinotas, and B. Ottersten, "Symbol-level multiuser MISO precoding for multi-level adaptive modulation," *IEEE Trans. Signal Process.*, vol. 16, no. 8, pp. 5511–5524, Aug. 2017. [Online]. Available: http://arXiv:1601.02788

[40] *IEEE P802.11 Wireless LANs, TGn Channel Models*, IEEE Standard 802.11-03/940r4, May 2004.

[41] *Evolved Universal Terrestrial Radio Access (E-UTRA); Physical Layer; General Description, Release 11*, document 3GPP TS 36.201, V11.1.0, 2008.

Muhammad R. A. Khandaker, photograph and biography not available at the time of publication.

Christos Masouros, photograph and biography not available at the time of publication.

Kai-Kit Wong, photograph and biography not available at the time of publication.